Headquarters
United States Army Accessions Command
90 Ingalls Road
Fort Monroe, Virginia 23651-1065
8 April 2005

USAAC Regulation 25-2

Effective 30 April 2005

Information Management: Management of Subdisciplines

Information Assurance

For the Commander:

ROBERT P. LENNOX
Brigadier General, US Army
Deputy Commanding General/Chief of Staff

Official:

ROGER H. BALABAN
Chief Information Officer

History. This UPDATE publishes a new USAAC Reg 25-2, which is effective 30 April 2005.

Summary. This regulation provides procedural, technical, administrative, and supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data.

Applicability. This regulation applies to any agency and all personnel accessing the United States Army Accessions Command and its subordinates automated information systems, to include contractors who operate Government-owned or contractor-owned automated information systems that process or store Accessions Command information. Contractors who process sensitive but unclassified information on contractor-owned automated information systems are governed by this regulation and the requirements in AR 25-2 if they connect to an Accessions Command automated information system and/or network system. All of the above must comply with all Department of Defense and Department of the Army regulations and Accessions Command requirements for accessing or utilizing Accessions Command automated information systems. During mobilization, deployment, or national emergency, this regulation remains in effect without change.

Proponent and exception authority. The proponent of this regulation is the Chief Information Officer. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. Proponent may delegate the approval authority, in writing, to a division chief within the proponent agency in the grade of GS-14.

Army management control process. This regulation contains management control provisions in accordance with AR 11-2 but does not identify key management controls that must be evaluated.

Supplementation. Supplementation of this regulation is prohibited.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ USAAC, ATTN: ATAL-IS, 1307 3rd Avenue, Fort Knox, KY 40121-2725.

Distribution. This regulation is available in electronic media only and is available on the USAAC Homepage at http://www.usaac.army.mil.

Contents (Listed by paragraph number)

Chapter 1
Introduction

1-1. Purpose

This regulation introduces and summarizes the United States Army Accessions Command's (USAAC's) approach to information assurance (IA). It applies to information systems (ISs) processing unclassified, sensitive but unclassified (SBU), and classified information. By using this information, system planners and organizational managers (e.g., designated approving authority (DAA), information assurance program manager (IAPM), information assurance network manager (IANM), information assurance network officer, information assurance managers (IAMs), information assurance security officers (IASOs), system administrators (SAs), and end users will have a common understanding of IA principles, concepts, and interrelationships.

1-2. References

For required and related publications and prescribed form see appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. IA Program

a. The USAAC IA Program is designed to comply with the National, Department of Defense (DOD), and Department of the Army (DA) IA policies. These policies stipulate that security must be considered throughout the life cycle of ISs. Requirements derived from these policies guide the development of products, techniques, and capabilities to satisfy USAAC IA objectives and to promote the implementation of innovative ISs technology. The USAAC IA Program has the following objectives:

(1) Employ efficient procedures and cost-effective, information-based security features on all information technology (IT) resources procured, developed, operated, maintained, or managed by USAAC organizational elements to protect the information on those resources.

(2) Protect the confidentiality, integrity, availability, authenticity, and nonrepudiation of information and resources to the degree commensurate with their value, as determined by the

required level of IA, classification or sensitivity level, and the consequences of their exploitation or loss for a period required by the mission supported.

(3) Conduct an assessment of threats, identify the appropriate combination of safeguards from the IA disciplines, and apply an appropriate Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) for each specific IS developed by a program office and for each local site employing networks and deployed ISs.

(4) Adopt a risk-based life cycle management approach in applying basic minimum uniform standards for the protection of USAAC IT resources that produce, process, store, or transmit information.

(5) Establish standardized IA training within USAAC.

b. DA policy is that all information and ISs shall be protected by the continuous employment of appropriate safeguards. This means that all USAAC ISs must provide some combination of confidentiality, integrity, availability, authenticity, and nonrepudiation protection mechanisms or procedures. Therefore, ISs must employ features to ensure that only authorized users who require access may access the information and/or resources when required.

c. Army ISs process, store, and transfer large quantities of information critical to its warfighting and support missions. Internetworking of ISs has expanded rapidly in the last decade and has resulted in newly integrated distributed networks with multiple worldwide uses. The information flow among these systems will continue to expand rapidly as systems are further integrated under the Global Command and Control System architecture and connected via the National Information Infrastructure and the Defense Information Infrastructure (DII) backbones.

d. The expected outcome of these IS advances is universal access to any information as permitted by security access controls. These advances in IS capabilities and information flow have also increased the vulnerability of DOD ISs to exploitation by both accidental exposure and malicious threat agents.

e. The IA challenge, to protect information in this new environment, has required a reorientation from stand-alone security approaches. The traditional, stand-alone, component-oriented approaches are being replaced with a fully integrated system security approach (i.e., a layered defense strategy) that combines all IA disciplines, as well as user awareness and knowledge to handle information and operate ISs in a manner which supports IA. The focus of the Army IA Program is to provide sufficient security to reduce the risk to IS assets to acceptable levels. Therefore, the USAAC goal is to employ the necessary safeguards to reduce and maintain the risk to its IS assets to acceptable levels.

Chapter 2

Policy

2-1. Properties of IA

a. Information and ISs must be properly managed and protected as required by law, regulation, or directive. IA is a composite of the properties addressed in this chapter and the services derived from them. When these properties are associated with other criteria, specific information security services (or functions) are provided. For example, ensuring the integrity of the information, which distinguishes one user from another, provides identification. Protection shall be achieved through the cost-effective, risk-balanced use of the IA disciplines, based on the level of IA required. Facilitating the management and protection of resources requires the appropriate implementation of security measures to ensure adequate system protection to support the IA properties identified in this section.

b. All USAAC information and resources shall be appropriately safeguarded at all times to support its missions. Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, authenticity, and nonrepudiation based upon mission criticality, level of required IA, and classification or sensitivity level of information entered, processed, stored, and/or transmitted. The safeguarding of information and ISs shall be accomplished through the employment of defensive layers that include the IA disciplines.

c. To ensure its safeguards and systems compliance with all DOD and DA regulations the following actions are required for contractors operating, accessing, or utilizing automated information systems (AISs) connected to a USAAC AIS and/or network system.

(1) USAAC shall provide AISs and services and/or IT necessary to perform the contract.

(2) All statements of work (SOWs) shall stipulate that USAAC provide the required AISs and services for performance of the contract.

(3) All SOWs shall stipulate that contractors who operate Government-owned or contractor-owned AISs that process or store Army information on contractor-owned AISs are governed by and must comply with DOD, DA, and USAAC IA regulations and requirements (to specifically include personnel background surety investigations).

(4) Should other requirements prohibit or make it impractical for USAAC to provide requirements, as above, the SOW shall stipulate that the contractor must comply with all DOD and DA regulations and USAAC requirements for accessing or utilizing Government AISs (to specifically include personnel background surety investigations and system accreditations).

d. Confidentiality. Confidentiality is assurance that information is not disclosed to unauthorized persons, processes, or devices. It is not limited to the protection of sensitive user information, but includes protection of security-relevant system information. For example, a system's password file should be hidden from general users. Confidentiality is typically implemented using several types of protection, including cryptography and access controls.

e. Integrity.

(1) Integrity is the quality of an IS reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms.

(2) Integrity supports the assurance that information collected, processed, stored, transferred, displayed, and/or disseminated within a system will not be accidentally or maliciously manipulated, altered, and/or corrupted, usually via an access control mechanism.

(3) Integrity functionality supports the ability to detect information that has been altered, either unintentionally or maliciously. Integrity has traditionally focused in two areas, data integrity and system integrity.

(a) Data integrity is the condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

(b) System integrity is the quality of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

(c) Software integrity security functions may also be used to protect software from undetected and unauthorized modification, manipulation, and/or destruction. As with data, the software may also have check sums or other integrity validation methods instituted to verify its integrity.

f. Availability. Availability supports the assurance of timely, reliable access to data and ISs for authorized users, and precludes denial of service or access. Accessibility and reliability of the system contribute to availability and provide assurance of continuity of operations. Availability-focused countermeasures protect against malicious logic and code, degraded capabilities, and denial of service conditions.

2-2. Information sensitivity categories

a. Information is categorized by its sensitivity to unauthorized disclosure, based on the effect on national security interests or other public interest concerns. To aid in the understanding of its need for protection this regulation will only define two categories of sensitivity, classified and SBU. All USAAC ISs, regardless of classification or sensitivity, shall implement appropriate security mechanisms and procedures to ensure IA.

b. Classified. Classified to the appropriate level to protect against unauthorized disclosure in the interests of national security, depending on the degree of damage to national security that the unauthorized disclosure would cause. Levels of classification are Unclassified, Confidential, Secret, and Top Secret.

c. SBU information. Sensitive information is any information which the loss, misuse, unau-

thorized access to, or modification of could adversely affect the national interest, the conduct of Federal programs, or the privacy of DOD personnel, but that has not been specifically authorized to be kept classified. Unclassified national security information, Privacy Act data, personal information (such as medical records, fitness reports, and performance evaluations), proprietary data, source selection data, and operational or mission information is considered sensitive information.

2-3. Mission critical system categories

a. Assessing the security requirements of any IS for IA properties requires a determination of the criticality of the system to the organization's mission, particularly the warfighter's combat mission. Two categories of criticality are defined, although an IS may have components that fit in both categories.

b. Administrative. Systems handling information that is necessary for the conduct of the day-to-day business, but does not materially affect support to the USAAC mission to, "field the force - from first handshake to first unit assigned."

c. Mission support. Systems handling information that is important to the support of the USAAC mission to, "field the force - from first handshake to first unit assigned." Information determined to be vital to mission effectiveness in terms of content and timeliness. (Information must be accurate, but can sustain minimal delay without seriously affecting mission effectiveness.) Mission support may include systems in direct support of systems that, if not functional, would preclude USAAC from conducting the full spectrum of its missions.

2-4. IA requirements

a. The types of IA protective measures, techniques, and procedures needed for a system shall be determined based on both information sensitivity and mission criticality. In general, higher levels of assurance are required for higher levels of system criticality and information sensitivity. The specific combination of measures to reduce risk shall be based on the analysis of threats and vulnerabilities, including system interconnectivity, and specific assurance needs as determined by the appropriate DAA, who will apply the principles of risk management. This requires a systematic process that identifies assets, threats, vulnerabilities, and risks to the system and selects risk mitigation approaches and countermeasures appropriate to the level of criticality and sensitivity of the system.

b. The purpose of the certification and accreditation (C&A) process is to determine whether the safeguards selected and implemented for an IS are adequate to protect the information and the system. This process follows the guidance provided in DODI 5200.40. DITSCAP activities are tailored to the specific requirements of the DAA and the considerations of mission criticality, sensitivity, risks, threats, vulnerability, and system interconnectivity.

Chapter 3
Risk Management Approach

3-1. General

a. Protection of IT resources requires a balanced, risk-based approach, managing the requirements of the system or resources with a cost-effective application of technical and nontechnical security disciplines and technologies to identify, measure, control, and minimize security risks to a level commensurate with the value of the assets protected.

b. Formal risk assessments for USAAC ISs and resources may be tailored, at the direction of the DAA, to the criticality and level of the IA threat. The Army IA Program is a fully integrated system security approach that helps reduce security risk in ISs. The integrated IA approach includes:

(1) Identification of all resources that support a system's ability to collect, process, store, transmit, display, and/or disseminate information.

(2) The identification of threats that may exploit a system security weakness or threat that make a system vulnerable, need to assessed to determine how IA can reduce risks to USAAC information and resources.

(3) Measurement of risk, a combination of the likelihood and the cost associated with exploitation. The likelihood of exploitation increases as the motivation, knowledge, skills, and abilities of a potential threat agent increase. The cost of exploitation increases based on the assessed value of the information, impact on mission, and the loss of resources or access to data systems associated with unauthorized disclosure, destruction, or modification of data.

3-2. Identification of assets

a. Achieving IA Program objectives requires identification of system resources and their vulnerabilities to specific threats. In reviewing a system's IA posture, information, hardware, software, communications, and personnel documentation resources should be considered. These resources provide the capabilities for a system to collect, process, store, transfer, display, and disseminate information. Each resource should be considered in relation to the system's operation mission and threats.

b. Information. The value of information to direct and indirect users is measured by its impact and/or use in terms of life, safety, mission, money, etc. The application of IA, based upon its value, ensures that information is protected from unauthorized disclosure or modification and is available when needed. Information in a system exists in one of three states:

(1) Processing. Information in the processing state is being manipulated by the IS.

(2) Storage. Information in the storage state is being maintained by the IS on storage devices such as a register, memory, disk, tape, compact disk-read only memory, or programmable read-only memory.

(3) Transfer. Information in the transmission state is being sent from one component to another. These components could be processors, networks, or auxiliary devices such as transducers, printers, and storage devices.

c. The goal of the USAAC IA Program to protect information applies regardless of its state.

d. Hardware. To protect the information that is collected, processed, stored, transferred, displayed, and/or disseminated by an IS, it is necessary to protect the hardware performing these functions. If unauthorized persons are able to gain access to the hardware, such as the central processing unit or disk drives (internal or floppy disks), they could make unauthorized changes that might cause the hardware to:

(1) Allow unauthorized disclosure of the information by writing the information to another file that could later be retrieved.

(2) Allow unauthorized modification of the information that would send incorrect information to a recipient.

(3) Create a denial-of-service situation that would prevent authorized users from gaining access to the information required to perform their duties.

e. Software. A system's software (including firmware) must be protected to ensure the integrity of the designed security mechanisms and the information being collected, processed, stored, transferred, disseminated, and/or displayed. Software needs to be protected during development, while it is being distributed to the system, and during operational:

(1) Development. Ensure that unintentional errors or malicious software are not introduced during software development and ensure adequate protective features are engineered into the design to protect system software and data during product operations.

(2) Distribution. Ensure that software sent from a facility, agency, or manufacturer to USAAC or from USAAC to any of its systems arrives at the system unchanged.

(3) Operational use. Ensure that unintentional errors or malicious software are not introduced into the system.

(4) Software that needs to be protected includes operating systems, system utilities, and application programs. Essentially, any software that has the ability to access the information must be protected to ensure that it performs only authorized actions on the information. Any unauthorized changes to the software could have the same results as those caused by changes to the hardware described in d above.

f. Communications. For an IS to be of value, users need to be able to communicate with the system and transfer information to other users and other systems. The communication path itself must prevent unauthorized access to the protected information and resources. The user's workstation may connect directly to a system through a modem or via a network (either local area network or wide area network (WAN)). Regardless of the specific mecha-

nism used to communicate with the IS, it is essential that the user be assured that information can be transmitted when required, with confidentiality and data integrity ensured.

g. Personnel. Personnel are critical to the correct operation of ISs. System and security administrators ensure that the system is configured and working properly and establish and define ISs operational and security policy and procedures. Supervisors and managers ensure that the user has the appropriate system access to perform his or her duties and to monitor user compliance with operational and security policy and procedures. Users both receive the system information and use the system to perform their duties. User error, improper use, and/or intentional misuse of the system by any of the personnel may result in disclosure, unauthorized modification, and/or denial of service through degradation of the information or the system itself. All of the personnel working with the system must be trained in system operations and be aware of general security threats to ensure effective and secure use of the system and its information. All personnel working with the system must receive an initial IA security briefing, have the appropriate completed background surety investigation, least privilege access, job and mission requirement, and the need to know to process, store, and/or transfer the information.

h. Documentation. Documentation that describes the hardware and software of the IS is critical to its proper operation and maintenance. Documentation supporting the hardware and software is necessary to:

(1) Describe the system's security features.

(2) Maintain the system in its current operational state.

(3) Recreate the system if critical assets are destroyed and an alternate measure must be used.

(4) Describe the risk associated with operating the system and plan improvements to the system, including security improvements, as technology permits.

3-3. Threat assessment

a. NSTISSI 4009 defines threats as any circumstances or events with the potential to cause harm to an IS in the form of disclosure, adverse modification of data, and/or denial of services. Threats are those circumstances with the potential to disrupt a system's confidentiality, integrity, availability, authenticity, and/or nonrepudiation properties. The following are examples of prominent systemic threats:

(1) Browsing.
(2) Misuse.
(3) Penetration.
(4) System flaws.
(5) Component failure.
(6) Tampering.
(7) Eavesdropping.
(8) Message stream modification.
(9) Denial of telecommunications.

b. A threat agent must initiate these threats. A threat agent can range from an individual to a nation state seeking to disclose, modify, and/or deny information and/or resources. Recent trends in identifying threats have indicated the greatest threat to DOD ISs is from an authorized source (i.e., the insider). The motivation of the threat agent can range from pure curiosity (i.e., "Can I get away with this?") to a nation state attempting to produce an unauthorized transfer of classified information and/or technology.

c. In the measurement of risk, the USAAC IA Program is focused on those threats that result from human agency, whether intentional or inadvertent. Unless availability is a highly critical assurance property of the IS, protection against normal service interruptions and preparation for natural disasters is the purview of continuity of operations planning and disaster recovery planning.

3-4. Vulnerability assessment

a. NSTISSI 4009 defines vulnerability as a weakness in an IS, cryptographic system, or components (e.g., system security procedures, hardware design, and internal controls) that could be exploited. Vulnerabilities of an IS are identified through demonstration, inspection, and/or analysis. Demonstration, inspection, and analysis activities occur throughout the life cycle of the IS. These activities begin early in the IS's development cycle through analysis of the system description documents to aid in the identification of appropriate countermeasures. Vulnerability assessment occurs throughout the design and development. Vulnerability assessment also occurs during the operational life of the IS to determine the current security posture. The weakness of an IS can be conveniently categorized as either technical or nontechnical in nature.

b. Technical vulnerability. Technical attacks are those that can be perpetrated by circumventing or nullifying hardware and/or software protection mechanisms, rather than by subverting system personnel or other users. The weakness in the hardware and/or software protection mechanism is the technical vulnerability that can be exploited by a threat.

c. Nontechnical vulnerability. Nontechnical vulnerabilities are those weaknesses in policy, procedures, personnel, and physical security that can be exploited to gain access to protected information and/or resources.

3-5. Measurement of risk

a. Risk is the probability that a particular threat will exploit a particular vulnerability of the IS. Risk probability is a measurement of the system vulnerabilities and motivation to exploit the vulnerability. Motivation is based upon the threat agent's capabilities to exploit the vulnerability through current knowledge, skills, or abilities, likelihood of being detected, and the value of the information and/or resource to be acquired.

b. Risk also includes an analysis of the likelihood that a threat occurrence will result in an adverse impact and assesses the severity of the adverse impact. Determining that the measured risk for an IS is acceptable is the final factor in determining if a system may be used operationally. A risk determination is required because it is nearly impossible to completely correct all vulnerabilities associated with an IS.

c. The risk assessment will indicate what the vulnerabilities are, determine the likelihood that threats will exploit a given vulnerability based on knowledge, technologies, resources, probability of detection, and the payoff, and predict the potential impact to the system if the vulnerability is exploited. Given all the factors in the risk equation and the cost of implementing countermeasures, a determination may be made that the risk potential of a given vulnerability is not worth the cost of correcting or implementing a countermeasure.

Chapter 4
Countermeasures to Risk

4-1. General

To mitigate the risks associated with operating an IS and to ensure the confidentiality, integrity, availability, authenticity, and nonrepudiation of the information and/or resources, IA countermeasures and sound security engineering need to be implemented. The information below introduces the IA disciplines and activities that can be used to implement appropriate countermeasures to the identified measurement of risk.

4-2. IA disciplines

a. Required levels of IA shall be achieved via a layered defense strategy, incorporating appropriate safeguards. Both technical and nontechnical security measures can assist in mitigating risk, and as such, shall be integrated into a cohesive program with the objective of protecting information and ISs. Appropriate countermeasures provided by these disciplines shall be applied to each USAAC IS and site security policy, through an assessment of the capability, probability, and motivation of a threat agent and the risk resulting from unauthorized disclosure, alteration, or nonavailability of information or resources to the mission. Information entered, processed, stored, or transmitted shall not exceed the approved classification or sensitivity level for the system or network. Use of the IA disciplines shall be carefully managed, regularly reviewed, and continuously monitored throughout the life cycle of IT resources.

b. Technology can be implemented in hardware or software components. A technical IA discipline could be as simple as a user identification and password used by the operating system or as complex as a smart card used for identification and authentication of a user. Typically, technology measures are thought of as supporting information security (INFOSEC), (communications security (COMSEC) and computer security (COMPUSEC)).

c. Policy and procedures are vital IA measures. A strong, enforced security policy pro-

vides the basis for all system security. Likewise, strong procedures that are followed, and thorough security education, training, and awareness complement the technical disciplines. Procedures and training help ensure that technology is used correctly. Procedures and training can also ensure that security mechanisms not addressed by technology are addressed through other measures. For example, procedures may be in place to ensure that only authorized personnel have physical access to a workstation connected to an IS. Other procedural measures may include a requirement for alphanumeric passwords of a minimum size and frequent password changes.

d. Policy and procedure measures are not likely to be effective if involved personnel do not know they exist or how they are used. Training and awareness measures must be in place so that all IS users know the technology measures in place and the policies and procedures that must be followed. Effective training and awareness measures will ensure that all personnel associated with the use, maintenance, and operation of an IS are aware of the technical and procedural security measures that are in place to protect the information. System administrators need to be trained to configure the system and options correctly so that the information and system resources are provided the necessary protection. Users need to be trained in the correct use of the security measures.

e. Additionally, an awareness program helps ensure that all personnel associated with the use, maintenance, and operation of an IS are aware of the general threats that are applicable to the system and the measures required to mitigate the threats. An awareness program can be one method to ensure that all personnel who work with the IS understand INFOSEC policy and procedures.

f. An active training and awareness program shall be incorporated at USAAC that includes all levels of system interaction (i.e., SAs, IA personnel, IT users, etc.,) for its various IT systems.

g. IA disciplines emcompass:

(1) COMSEC. COMSEC provides protection through measures designed to deny unauthorized individuals information that might be derived from the possession and study of communications. National Security Agency (NSA) approved COMSEC products, techniques, and protected services shall be used, as required, to secure USAAC communications. Products validated by the National Institute of Standards Technology or NSA shall protect sensitive information. Virtual private networking techniques, incorporating commercial-off-the-shelf or Government-off-the-shelf products are also available, and shall be incorporated as appropriate.

(2) COMPUSEC. COMPUSEC provides IA through measures designed to obstruct deliberate or inadvertent disclosure, modification, unauthorized use, loss of information, or denial of service to users. COMPUSEC technical measures, applied via a combination of hardware and/or software solutions, shall be employed as appropriate.

(3) Emanations security.

(a) Electronic communications can produce unintentional, intelligence-bearing emanations that, if intercepted and analyzed, may disclose information transmitted, received, handled, or otherwise processed.

(b) Any USAAC requirements for TEMPEST countermeasures shall be employed in proportion to the threat of exploitation and the associated potential damage to national security, as recommended by a DA certified TEMPEST technical authority which provides specific objectives for reducing or eliminating unintentional emanations.

(4) Personnel security. Personnel security provides a level of assurance that an individual's access to USAAC information and resources is based on the person's loyalty, reliability, and trustworthiness, such that the person can be entrusted to perform their duties. Based on assigned duties and need to know, personnel accessing USAAC AIS shall undergo an appropriate background check as directed by AR 25-2. Individuals shall not be granted a clearance for access to information classified higher than needed to accomplish their assigned duties. Access by non-US citizens, foreign nationals, or representatives of foreign entities shall be governed and provided in accordance with AR 380-67.

(5) Physical security. Physical security is the action taken to protect USAAC IT resources (e.g., equipment, electronic media, and documents) from damage, loss, theft, or unauthorized physical access. Commanders, directors, and/or supervisors and managers are responsible for ensuring the physical security posture is accurately assessed and security resources are appropriate to protect USAAC information and resources.

(6) Procedural security. Procedural security, including operations security measures, can provide an alternative to technical security means when risk analysis indicates the use of procedures does not increase the overall risk to a system or network. Procedural security provides the necessary actions, controls, processes, and plans to ensure operation of a system or network within an accredited security posture, and is site and task dependent. Site security procedures shall be developed to supplement the security features of the hardware, software, and firmware of IT resources, to include such standardized processes as user access control, media labeling, and material marking and handling.

(7) Security Education, Training, and Awareness Program (SETAP). The goal of SETAP is to develop fundamental habits of security such that proper discretion is ingrained in the security and conduct of duties for USAAC IT resources. Commanders, directors, and/or supervisors and managers shall ensure every individual under their cognizance receives the appropriate level of SETAP commensurate with their assigned duties. Initial IA awareness indoctrination and annual IA security awareness updates shall be provided to all military, civilian, and contractor personnel who access, manage, or use USAAC IT resources in any system life-cycle phase. In addition, all individuals assigned, performing, or designated as INFOSEC professionals shall receive basic and system specific training commensurate with assigned duties and responsibilities and recurring, refresher or follow-on training annually to maintain their skills and proficiencies.

4-3. Risk mitigation activities

a. IA encompasses more than INFOSEC, but INFOSEC is at the heart of protecting USAAC information assets. INFOSEC includes active, passive, and reactive measures to prevent, deter, limit, and detect internal and external security violations and reduce vulnerabilities. The activities listed here include both procedural and technical safeguards; encompass multiple dimensions of IA disciplines listed above; and should be considered essential components of any INFOSEC posture.

b. System security authorization agreement (SSAA). The approach to the C&A process is documented in the SSAA, a formal agreement between the DAA, Certification Authority (CA), user or site representative, and program manager (PM). Used throughout the C&A life-cycle phases, the SSAA documents decisions, specifies IA requirements, documents required level of C&A, identifies possible solutions, and documents operational system security. The SSAA consolidates security-related documentation into one document and may be tailored as appropriate. An SSAA shall be developed for each site or system being accredited.

c. Policy, standards, and procedures.

(1) As part of the C&A process, an information system security policy shall be developed and maintained for each IS. The information system security policy shall identify the security requirements, objectives, and policies implemented to safeguard the site or system in a prescribed operational configuration.

(2) Failure to implement sound security procedures during system design may compromise the effectiveness of other security mechanisms, such as packet filtering routers and firewalls. Although it may appear that appropriate security features have been incorporated at the individual system level, unanticipated vulnerabilities may surface when operating with other systems over shared communication links. The DAA must consider the inherent risk of operating less secure systems inside a secure enclave. To the extent possible, legacy systems shall employ system security standards that support appropriate security protocols within a secure enclave. Modifications to legacy systems should prioritize incorporation of common security procedures and products to improve their overall security postures. Those legacy systems with unsecured security implementations should be placed outside the secure en-

clave or in a separate "safe" zone if they pose significant security risks to other information resources protected within the enclave.

(3) Consistent, clearly documented operating procedures for both system configuration and operational use are key to ensuring IA. Procedures should define deployment of the system, system configuration, day-to-day operations for both the SA and user, as well as how to respond to real or perceived attempts to violate system security. All USAAC ISs and networks shall include written standing operating procedures, which are routinely updated and tailored to reflect changes in the operational environment.

d. Configuration management.

(1) Configuration management identifies, controls, accounts for, and audits all changes made to a site or IS during its design, development, and operational life cycle. Proper configuration management can substantially reduce and sometimes eliminate the need for costly complete reaccreditation. Appropriate levels of configuration management shall be established to maintain the accredited security posture. Each change or modification to an IS or site configuration shall assess the security impact of such a change against the security requirements and the accreditation conditions issued by the DAA.

(2) Official business shall normally be conducted using Government-owned resources. Policies and procedures shall be established controlling the use of personal hardware and software, to include the use of antivirus software. Processing of classified information using personally-owned hardware and software is specifically prohibited. USAAC personnel shall not use personally-owned IT resources to conduct official business without specific, case by case, prior written authorization of the DAA, who shall ensure appropriate security procedures against viruses and for protection of sensitive information. The appropriate security procedures shall be identified within the contract for handling and disposal of information and IT resources. Software that is personally procured, developed, or obtained as "public domain" or "shareware," shall not be installed on Government-owned systems without the IAM's, IASO's, and/or SA's evaluation for compatibility, correct operation, and absence of viruses.

e. Acquisition management. USAAC shall apply appropriate resources to ensure cost-effective IA measures are incorporated in each acquisition program. Army PMs are responsible for the accomplishment of all activities and tasks associated with security certification leading to accreditation of the system under their developmental responsibility. The security test and evaluation plan shall also specifically address system security certification testing plans and requirements.

f. Multilevel security, multiple security levels, and interoperability.

(1) USAAC operational missions may require interoperability between ISs operating at different classification or security levels. Application of unsecured solutions and the improper implementation of secure solutions can introduce vulnerabilities that require mitigation.

(2) Requirements for secret and below multilevel interoperability shall be validated in accordance with Assistant Secretary of Defense Memo, Secret and Below Interoperability, and acceptable solutions, employing approved products, shall be engineered.

(3) All systems that share information between different classification or security levels shall be specifically documented in the SSAA and accredited by the appropriate DAA prior to operation.

g. Contingency planning. Given the dependencies of today's operations on IT resources, all USAAC systems must be prepared for worst-case contingencies in the event of the nonavailability of ISs and resources or denial of service conditions. System and network design should incorporate redundancy and data backup in accordance with the level of IA required. Contingency plans shall be developed and tested to prepare for emergency response, backup operations, and post-disaster recovery. At a minimum, contingency planning shall address reconstitution for the loss of processing, storage, or transmitting of information.

h. Security incident procedures. In addition to protective measures designed into ISs and architectures, sites should have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of USAAC operations.

i. Consent to monitoring. All individuals attempting access to USAAC ISs shall be provided sufficient notice that use of official DOD ISs or networks constitutes consent to monitoring. Adequate warning shall be provided by clearly displaying the legally-approved DOD warning banner. At a minimum, the DOD warning banner shall be displayed to the user upon initial entry or login to system, network, local, and remote resources. Acceptance of the banner-warning screen shall constitute consent to monitoring. The approved warning banner is available in AR 380-53 and AR 25-2, which also provides additional information and guidance on monitoring.

j. Network management tools. Network management tools that detect, isolate, and react to intrusions, disruption of services, or incidents that threaten the security of USAAC IT resources shall be used.

k. Army computer emergency response.

(1) The Army Computer Emergency Response Team (ACERT) serves as the Army's primary computer incident response capability to provide assistance in identifying, assessing, containing, and countering incidents that threaten ISs and networks. USAAC will collaborate and coordinate ACERT efforts and with other Government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and ISs, and to minimize or eliminate identified vulnerabilities.

(2) Incident reporting. USAAC shall promptly report incidents that threaten DOD information and resources to the ACERT. This reporting requirement does not preclude commanders from establishing parallel reporting requirements within their assigned area of operations nor does it alleviate or replace any additional reporting requirements established by the chain of command. The following types of incidents shall be reported:

(a) Computer intrusions. Unauthorized access to data or to an IS.

(b) Attempted intrusions. Unauthorized, unsuccessful attempts to access data or an AIS.

(c) Denial of service attacks. Actions which prevent any part of an AIS from functioning in accordance with its intended purpose, to include any action which causes the unauthorized destruction, modification, or delay of service.

(d) Malicious logic. Hardware, software, or firmware that is intentionally included in an IS for an unauthorized purpose, such as a virus or Trojan horse.

(e) Probes. Any unauthorized attempt to gather information about an AIS or its users online.

(3) ACERT advisories. ACERT issues periodic advisories summarizing and highlighting computer incidents. USAAC system, site, and IT PMs shall review all ACERT advisories and ensure appropriate action to implement IA protections against vulnerabilities reported in the advisories.

(4) COMSEC material incident response. Incidents involving the compromise or the suspected compromise of COMSEC material or incidents that warrant further investigation shall be reported in accordance with procedures established in DOD and DA IA publications.

l. Vulnerability assessments. Assistance is available to assess and improve the IA posture, by identifying vulnerabilities in an operational environment and validating a particular site's overall security posture and degree of system integration. Requests for IA assistance visits should be forwarded to the DAA or IAPM.

m. IA assistance visits. USAAC will provide for the availability of IA assistance visits designed to provide assistance in the identification and subsequent safeguarding of IS vulnerabilities.

n. ISs infrastructure interconnections. Networked ISs may incur additional risks because of the exposure of their data and resources to a larger community of users. Assessing benefits and risks of internetworking, as compared with the costs to mitigate and control risks, is required as part of the overall vulnerability analysis. Decisions to maintain connections to other networks should be made with awareness of the lack of control over the security safeguards in use by other network infrastructures. Use of products that have been certified under FIPS Pub 140-2 is encouraged, both to reduce the burden of additional certification and to provide incentive for industry to provide products that comply with the standards.

(1) DII. USAAC's connections to the DII (including the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET)) shall be coordinated in accordance with established Defense Information Systems Agency requirements. Appropriate protections shall be employed in a Defense in Depth approach to protect the associated data and systems.

(2) National Information Infrastructure. USAAC's systems that connect directly to non-DOD infrastructures, such as the Internet, shall apply appropriate security technologies, to specifically include a firewall, to protect IT resources from unauthorized external activities.

(3) Remote control and management. Remote control or remote management software protocols that are used across these boundaries shall be discontinued except via approved access assurance means, such as strong authentication (e.g., one-time passwords or X.509 certificates).

(4) Web site operations. USAAC's information servers and services established and maintained on WANs (such as the Internet, NIPRNET, and SIPRNET), including World Wide Web sites, must support legitimate, mission-related activities and be consistent with prudent operational and security considerations. The goal is to provide maximum availability at acceptable levels of risk, with sufficient access and security controls.

(a) Classified information shall not be posted on publicly accessible web servers. Access to classified or SBU information via the SIPRNET or NIPRNET shall be controlled by strong authentication or encryption.

(b) Internet web servers shall be hosted within a separately protected demilitarized zone (DMZ). A DMZ is a dedicated network segment used to separate public services (such as e-mail or web servers) from internal services. It should be protected by a different firewall than the internal network segment, or a separate interface on the existing firewall. If neither option is available, the DMZ should be outside the firewall. USAAC shall only use Internet web-hosting services provided by a centralized Network Operations Center. Intranet and Extranet web services shall be protected with appropriate access controls.

(c) Web servers connected to a WAN shall be specifically included and addressed in the site SSAA.

(d) Prior to final accreditation, appropriate procedures and mechanisms shall be established to ensure prompt detection of unauthorized access or modification to web servers and services, as well as contingency plans to ensure prompt restoration of capability as required.

(e) Each publicly accessible web information service shall provide a privacy and security notice to users upon initial access to the Web site in accordance with Office of the Secretary of Defense Policy for Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service.

(f) All files downloaded or received over a WAN shall be virus checked, using the command standard antivirus software with current virus definition files, prior to placing on a local workstation drive. Unless specifically authorized in the SSAA, files shall not normally be downloaded directly to a network or shared drive.

(g) Each Web index page shall have a designated author or maintainer, responsible for the content and appearance of the page. That individual's name, organizational code, organizational telephone number, e-mail address, and date of last revision shall be included in the source code for that page.

(h) Web sites hosted by commercial Internet service providers shall not normally be used for official purposes due to the inability to identify and directly control any implemented security measures. This policy does not preclude USAAC from contracting with a commercial organization to establish and host a Web site if appropriate security measures are maintained by the commercial organization contracted to provide this service. Outsourcing web services does not relieve the command of the responsibility to accredit the system.

(5) Firewalls. Firewalls are security products that control the flow of traffic between networks and offer security protections such as packet filtering, application proxying, access control, and stateful inspection. Firewall protection may be achieved via a specifically designed product, or through inherent capabilities within existing resources. Mere presence of a firewall does not ensure protection. The firewall must be configured correctly, based on the technical architecture of the operating environment and the overall security architecture, with sufficient access and security controls, policies, and procedures to protect information from unauthorized internal or external compromise. Firewall selection, engineering, configuration, and operation shall be in accordance with the Command Chief Information Officer's guidance.

(6) Remote access. Uncontrolled and nonsecure remote access to USAAC ISs and networks may bypass other system security measures. Sites with either dial-up or WAN remote access capability shall have adequate access controls and authentication procedures, commensurate with the classification or sensitivity level of the data and systems involved. Authentication procedures should verify the identity of the user, as well as control access to specific systems and data. The NSA, Defense Information Systems Agency, and Chief Information Officer provide guidance on the use of sophisticated access control mechanisms beyond simple password access control, such as one-time passwords, X.509 certificates, or authentication tokens. The legally approved DOD warning banner, available on the USAAC IA Web site, shall be displayed at the network and system level upon establishment of each remote access session.

(7) Mobile computing. Mobile computing poses issues of physical security, as well as remote access. Appropriate physical security measures shall be employed to protect the mobile hardware, software, and data contained therein, or data accessible via the mobile hardware, commensurate with the classification or sensitivity level of the data and systems involved. Specific safeguards, such as approved encryption mechanisms, should be employed to protect information in the event the mobile hardware falls into unauthorized control.

(8) Encryption. Encryption, when used correctly, can protect the security and classification of data during transmission and storage. Encryption can be employed at either the network level or the application level. There are numerous Government and commercial alternatives for employing encryption techniques. To ensure security and interoperability when using encryption, the USAAC IA Office shall be contacted for guidance prior to system design and for approval prior to employment.

(9) Certificate management. Properly employed public key based security mechanisms provide a good means to protect USAAC ISs from unauthorized access and to provide access control to system resources. Only approved workstations shall be used for certificate establishment and management services. Requirements for public key based digital signature and encryption services shall be implemented to ensure compliance with the DOD public key infrastructure policy as mandated in Deputy Secretary of Defense memo U07287/99 dated 6 May 1999, the PKI Roadmap for the DOD, and supporting DA guidance.

(10) Virus and malicious code protection.

(a) The threat of attack from computer virus or other malicious code, both deliberate and inadvertent, is significant. Successful virus prevention incorporates technical, policy, and procedural elements. All USAAC's ISs and networks shall use antivirus software to intercept viruses before they can establish themselves. The command shall develop and implement local policy and procedures to support effective employment of antivirus software.

(b) As the nature of the threat from virus software constantly changes, sites shall ensure that antivirus software profiles are updated frequently and on a routine basis. DOD licensed antivirus software is available free to all USAAC activities, and may be downloaded from the IA Web site (http://usarec.army.mil/im/SIO/IA/index.html). This software is also authorized for, and should be installed on, personal computers, privately owned by DOD personnel, used for official business.

(11) Data management. The increasing reliance on distributed, interconnected ISs negates many of the data protection mechanisms built into traditional contained "system high" networks and requires additional safeguards to protect USAAC information from both unauthorized users and from authorized users without a need to know. Data processed, transmitted, and stored

on USAAC's ISs shall be protected to the appropriate level of classification or sensitivity and required level of IA.

o. Data marking. Electronic data and files shall be marked to reflect the appropriate classification or sensitivity. At a minimum, all electronic information in the form of documents, images, or other human-viewable format, regardless of location, shall include plain-text markings indicating classification or sensitivity, as would be required if they were hard-copy products.

p. Data release. Data, both physical (e.g., hard copy) and electronic (e.g., floppy disks, web pages), shall be released in accordance with established DA data release procedures.

q. Data access. Appropriate procedures for establishing and disestablishing access and authentication shall be based on need to know and the classification or sensitivity level of the information. Authentication and access control may be enforced by the operating system or through encryption techniques.

r. Passwords. Passwords are one of the simplest, most effective security measures, but are often the first target of intruders. Passwords shall be managed in accordance with the below guidelines and tailored to the appropriate level of protection required.

(1) When passwords are the single authentication credential, they shall be a minimum of eight characters in length, consist of a mixture of alphanumeric characters (i.e., a-z, A-Z, and 0-9), and avoid the use of names and dictionary words. Legacy systems constrained by system design may be exempt from the eight-character minimum password length requirement, with the approval of the DAA.

(2) SAs should use available tools to evaluate the strength of passwords under their control.

(3) Accounts shall not be issued with default passwords (e.g., "password"). Default passwords at the system or network administrator level shall be changed to a site unique password upon system installation, and verified prior to final system accreditation.

(4) Access to password files shall be appropriately protected from unauthorized users.

(5) For systems with automated password administration capability password change shall be system forced semiannually, at a minimum. All other systems shall incorporate user training to advise users to change passwords semiannually, at a minimum. AR 25-2 and CSC-STD-002-85 provide additional information on password usage.

s. Account management. SAs shall monitor user account inactivity and establish procedures for investigating, deactivating, and eliminating accounts that do not show activity over time. For example, deactivate accounts with no activity for over 30 days, and investigate and eliminate accounts with no activity for over 90 days. Applicability and associated privileges of all default accounts shall be validated and deactivated, as appropriate, prior to system accreditation.

Chapter 5
Certification and Accreditation Requirements

5-1. General

All USAAC's ISs, as well as sites employing IT resources at the local level, shall be accredited for operation. Site accreditation should include the aggregate of all ISs, networks, and other resources used to support mission accomplishment. ISs developed or procured by a program office shall be accredited at the system and site level prior to deployment. Accreditation shall be achieved through the DOD C&A process as described in DODI 5200.40 and AR 25-2. Implementation of the C&A process may be tailored to fit the size and complexity of the system and the required level of IA. Key participants in the C&A process include the IAPM, the DAA, the CA, and the system's IA officer.

a. Certification.

(1) Certification is the comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. DOD has tailored the certification process that supports this definition of certification. Certification is a two-part process covering the definition, verification, and validation phases of the C&A process.

(a) A comprehensive evaluation of the technical security features of an IS to establish the extent to which a particular design meets a set of specified security requirements.

(b) A comprehensive evaluation of the nontechnical security features of an IS to establish the extent to which a particular implementation meets a set of specified security requirements.

(2) The first part, which assesses the technical security features, establishes the extent to which the developed IS (the target of evaluation) has applied the INFOSEC measures of COMPUSEC, COMSEC, and Emanations security. This assessment is against a developed product. This effort can be performed once, independent of a specific implementation, and the results reused many times. The CA states that a comprehensive evaluation of the technical security features of an IS has been conducted and establishes the extent to which a particular design meets a set of specified security requirements. This certification activity includes reviewing design documentation, performing design level risk assessments (used to determine compliance with a stated IS security policy), and conducting certification test and evaluation.

(a) Design documentation. Set of documents, required for the evaluation criteria for IT, whose primary purpose is to define and describe the properties of a system. Design documentation provides an explanation of how the security policy of a system is translated into a technical solution via the security functions of the hardware, software, and/or firmware.

(b) Risk assessment. Process of analyzing threats to and vulnerabilities of an IS and the potential impact the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and cost-effective countermeasures.

(c) Certification test and evaluation. Software and hardware security tests conducted during development of an IS. The purpose of these tests is to verify the technical security requirements have been correctly and completely implemented into the system.

(3) The second part, which assesses the nontechnical security features, establishes the extent to which a particular implementation meets a set of specified security requirements. This assessment is against a product implemented in an operational environment and is called "Operational Site Certification." This is a statement by the local authority certifying that the system has been installed in an approved configuration and in an environment that satisfies nontechnical INFOSEC measures. The operational site certification statement is made based upon the results of security test and evaluation. It is the formal examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of that system.

b. Accreditation.

(1) Accreditation includes a formal declaration by a DAA that a site or an IS is approved to operate in a prescribed operational configuration using a defined set of safeguards and countermeasures against stated threats and vulnerabilities. DAA responsibility for ISs developed or procured shall be assigned in accordance with AR 25-2.

(2) After the system has been certified, but before it can be placed into operation, the risks associated with operating the system must be assessed. The DAA participates in the development of and performs the final review of the SSAA (as explained below) and accredits or denies accreditation for the operation of the system.

(3) The set of safeguards discussed in the definition of accreditation are those traced back into the objectives of the IS security policy and validated through certification.

(4) The SSAA certifies the INFOSEC requirements that are designed and implemented into the IS and an assessment of the risk of operating the IS after all of the INFOSEC measures are put into place. The accreditation process is a risk management approach whose final action is to document the residual risk of operating an IS. Residual risk is that portion of the risk remaining after security measures have been applied.

(5) Upon completion of the accreditation process, the DAA may take one of the following four actions:

(a) Accredit the system to process information in the given operational environment.

(b) Issue an interim authority to operate (IATO). An IATO is issued when the DAA determines that changes must be made to the system or its environment, but the system will be allowed to operate in the interim. An IATO may not exceed 1 year.

(c) Reject accreditation and recommend enhancements that will lead to accreditation.

(d) Reject accreditation because of inherent security deficiencies and provide rationale.

(6) Accreditation must be reviewed when changes are made to system functionality, architecture, interfaces, information processed, environment, and user communities because these changes may increase the risk to the system.

5-2. Five phases of C&A

The C&A process is divided into five life-cycle phases:

a. Definition. During the definition phase, system mission and architecture are documented, potential threats and security requirements are identified, the DAA and CA are identified, and an overall approach to the certification process is developed.

b. Verification. During the verification phase, security activities are developed to verify compliance with the identified security requirements.

c. Validation. During the validation phase, the integrated system or site is validated in the designated operating environment against an acceptable level of risk. The validation phase ends with an approval to operate in an accredited security posture (i.e., accreditation).

d. IATO. When it is necessary for a site or an IS to become operational before the residual risk can be fully determined, an IATO may be issued by the DAA, for a period not to exceed 1 year. All available certification evidence normally considered for full accreditation shall be provided to assist in determination of the IATO. The IATO shall stipulate the remaining requirements to achieve accreditation.

e. Postaccreditation. The postaccreditation phase monitors the operational site or IS to ensure the accepted level of risk is maintained throughout the life cycle, to include changes in threat conditions, the application of new requirements, or changes to system configuration. Accredited sites and ISs shall be subject to periodic compliance reviews, as required by the DAA and specified in the SSAA. Specific timing and activities required for reaccreditation shall depend on the degree of change to the security posture of the site or system. A system must be reaccredited when significant changes have occurred or every 3 years, whichever comes first.

5-3. Certification levels of effort

a. The certification level of effort indirectly determines the amount of resources that will be expended on providing the DAA with the amount of information required to make an informed accreditation decision. The certification level of effort provides a uniform baseline for application of the INFOSEC C&A process on ISs with similar characteristics.

b. The specific level of effort and documentation for certifying a system is at the discretion of the DAA, based on specific factors that may increase or decrease the degree of certification testing, analysis, and documentation required. These factors include the degree of interconnection with other systems, the life expectancy of the system, and the cost of achieving the full level of effort associated with the certification. For example, a system with no system interconnections, limited life expectancy, and high cost to certify should not require the same level of effort as one with multiple interconnections, longer life expectancy, or lower cost to certify. Table 5-1 is provided as general guidance to aid the determination of the level of effort that should be applied to conducting the certification process.

c. Administrative checklist level of effort. This level of effort requires documenting the status of IA requirements and the technical, physical, and administrative safeguards as implemented. USAAC Form 106 (Security Requirements Checklist) should be used (see sample at fig 5-1) (for relatively simple IT systems, many items in the checklist may not be applicable).

d. Basic certification level of effort. Basic certification level of effort includes development of an SSAA, concept of operations, IS security policy, network topology map, and residual risk assessment.

e. Medium certification level of effort. Medium certification level of effort includes those task activities and documentation requirements from the basic IA level of effort and any additional documents negotiated with the DAA. These would normally include a more detailed evaluation of the system's development and lifecycle maintenance process and the safeguards to the integrity of system content throughout the life cycle.

f. High certification level of effort. High certification level of effort includes addressing all of the task activities and documentation requirements addressed in DITSCAP. This level of effort adds a more exhaustive evaluation of the internal functionality of elements of the system, such as the operating system, applications, utili-

Table 5-1
Certification levels

Level	Explanation
Administrative Checklist	The administrative checklist certification is the simplest certification to conduct. It involves completion of a minimum security checklist, which includes verification that procedures for proper operation are established, documented, approved, and followed. Minimal evidence is required for this type of certification.
Basic Assurance	The basic assurance certification is more extensive than Level A, and begins with completing the Level A checklist. The amount of documentation required and the resources devoted should be low. The focus of this type of certification is INFOSEC functionality (auditing, access control, identification, and authentication). Some documentary and test evidence is required for this type of certification.
Medium Assurance	The medium assurance certification is more detailed and complex and requires more resources. This type of certification is generally used for systems that require a higher degree of assurance, have a greater level of risk, and/or are more complex. The focus of this type of certification is also on INFOSEC functionality. However, more extensive documentary and test evidence is required to show that the system meets the security requirements.
High Assurance	The high assurance certification is the most detailed and complex and generally requires a great deal of resources. This type of certification is used for systems that require the highest degree of assurance and may have a high level of threats and/or vulnerabilities. The focus of this type of certification is INFOSEC functionality and assurance. Extensive evidence, generally found in the system design and test documentation, is required for this type of certification.

ties, and system interfaces. The ISs that are characteristic of this level of effort are those that are centrally procured and involve separation and protection of information at different classification levels or compartments.

5-4. INFOSEC certification assistance

Anyone can conduct the C&A process. These certification agents primarily focus on medium and high IA level certification efforts, whereas basic IA level of effort can be conducted by the INFOSEC personnel at the local site with guidance from the identified certification agents. The certification agents can and will assist the local sites in achieving their basic IA level C&A.

Chapter 6
Roles and Responsibilities

6-1. Organizational responsibilities

a. IA responsibilities are assigned to organizations and individuals within USAAC.

b. The Information Support Activity is responsible for ensuring the Army IA Program is implemented within USAAC in full compliance with DOD and DA regulations.

6-2. Individual responsibilities

The individual roles and associated responsibilities are located in AR 25-2. Roles and abbreviated responsibilities are:

a. DAA. The DAA is the management official who determines whether an IS can be operated with the known level of risk by accepting responsibility for that risk. The accreditation decision of the DAA is based on the operational need for and the threats to the system. The DAA must make an accreditation decision based on a trade-off between the operational need and the criticality of the system (and its information) against the risks posed by the known threats.

b. IAPM. The IAPM establishes and maintains the command's IA Program.

c. IANM. The IANM serves as the alternate IAPM and provides direct support to the IAPM on matters of Computer Network Defense and the command's IA Program.

d. IAM. The IAM is the IAPM's technical security advisor. The IAPM will rely on this individual in establishing and maintaining the command's IA Program. The IAM is responsible for a specific grouping of systems or sites.

e. IASO. The IASO is the IAM's technical security advisor. An IASO is appointed for individual systems or for a specific area or site managed by the IAM. IASOs are responsible for ensuring that appropriate technical and procedural measures are established for their systems or areas. These measures include a training and awareness program; access control to the hardware, software, and data; auditing user actions; system accreditation, a risk management program; and an adequate contingency plan.

f. Local information assurance security officer (LIASO). The LIASO assists the IASOs in performing their duties. Typically, the LIASOs are responsible for specific terminal, office, or work areas that are connected to the system.

SECURITY REQUIREMENTS CHECKLIST

(For use of this form see USAAC Reg 25-2)

SECURITY REQUIREMENT GUIDANCE	COMPLIANCE		
	MET	NOT MET	NA
Rules of behavior for system and application use shall be established. The rules should clearly delineate responsibilities of and expectations for all individuals with access to the system.	✓		
An information assurance security officer shall be assigned for each system with responsibility for security in writing, and be trained in the technology used in the system and in providing security for such technology.	✓		
The information assurance security officer shall obtain and maintain certification.			
CONFIGURATION MANAGEMENT	**MET**	**NOT MET**	**NA**
A system configuration management plan shall be developed for all system components.	✓		
Users are prohibited from installing freeware, shareware, or public software on the system without appropriate administrative oversight.	✓		
Software acquired through other than the appropriate procurement channels must be scanned for malicious code.	✓		
Procedures shall be established to ensure the correct versions of the hardware, software, firmware, and documentation are installed and available.	✓		
The distribution of security-related software, hardware, and firmware is properly controlled.	✓		
Users are prohibited from installing freeware, shareware, or public software on the system without appropriate administrative oversight.	✓		
Security software (e.g., firewalls, guards) and security-related software patches are not made operational until successful testing by the appropriate organization is conducted.	✓		
All security-related alert recommendations (e.g., from the Army Computer Emergency Response Team) are followed as soon as possible.	✓		
MEDIA CONTROL	**MET**	**NOT MET**	**NA**
Backup media shall be properly labeled with sufficient information (e.g., type of data, date of creation).			
When equipment or media are reused by a new user group, the storage media and nonvolatile memory devices must be cleared.			
Hard disks are cleared of sensitive information before being submitted for servicing.			
All magnetic media used to store sensitive unclassified information are cleared or destroyed when no longer needed.			
Purging and destruction methods for media must be approved in writing.			
IDENTIFICATION AND AUTHENTICATION	**MET**	**NOT MET**	**NA**
The system employs a method to identify uniquely all users of the system before allowing the users to perform any actions on the system and to maintain their identity throughout their active sessions on the system.	✓		
The system provides or incorporates a mechanism for authentication management and the authentication data are protected to prevent unauthorized or inadvertent access.	✓		
The system is able to provide hardware identification of remote terminals and personal computers.	✓		
Logon identifications must be uniquely identifiable.	✓		
The automated information system shall lock out an interactive session after an interval of user inactivity not to exceed 30 minutes.	✓		

USAAC Form 106, 1 Apr 2005 **V1.00**

Figure 5-1. Sample of a completed USAAC Form 106

User access shall be prohibited after a specific number of invalid login attempts (i.e., three times).	✓		
Null passwords are not accepted.	✓		
Passwords are not reusable by the same individual for a period of six password change iterations.	✓		
Protected system resources are only available to users after successful completion of identification and authentication.	✓		
Each data object in the system has an identifiable source (i.e., owner) throughout its life cycle.	✓		
All dial-up access to sensitive but unclassified automated information systems and telecommunications networks shall be protected with security measures that provide explicit user identification and authentication and audit trails.	✓		
Passwords are blotted out when entered.	✓		
ACCESS CONTROL	**MET**	**NOT MET**	**NA**
The principle of least privilege is used in allowing access to the system services.	✓		
All personnel associated with the system have the appropriate personnel security background investigation prior to being provided access to the system.	✓		
The system provides for the extraction of any data contained in its databases about an individual, in response to a request by that individual or his or her representative, when required by the Privacy Act.	✓		
The system provides a mechanism for user-initiated locking of interactive sessions.	✓		
The system provides a mechanism to limit the privilege a user may obtain based on means of access or port of entry.	✓		
Before initiating the system logon procedure, the system displays an advisory warning message to the user.	✓		
The system ensures that a user is not able to access the prior contents of a resource that has been allocated to that user by the system.	✓		
Access to the audit data is strictly limited.	✓		
The system, if connected to other networks, provides insulation (e.g., firewalls) to prevent unintended and/or unauthorized access from the Internet by "back-end" users.	✓		
Procedures and mechanisms are in place to protect against threats from connected networks operating at a lower security level than that of the local subscriber environment.	✓		
The equipment's operating system has built-in protection to prevent bypassing of security and the unauthorized access to data.	✓		
The system software restricts individual access to only the files and data for which the user is authorized.	✓		
Approval to enter data is obtained from the data owner, where applicable, and is authorized by management for entry.	✓		
When an individual who has been granted access to an automated information system no longer requires access privileges, the individual's identification, passwords, and other access controls shall be immediately removed from all systems.	✓		
Only necessary network services shall be run on servers.	✓		
The system is configured to protect resources from unauthorized access.	✓		
AUDIT	**MET**	**NOT MET**	**NA**
The system provides or incorporates an audit mechanism that maintains individual accountability of a subject's access to the objects the system protects.	✓		
The system provides or incorporates a mechanism for audit analysis. Audit trails are sufficient to identify individuals associated with security events.	✓		

Figure 5-1. Sample of a completed USAAC Form 106 (Continued)

The system provides other audit options for use when the standard audit mechanism is unable to record events.	✓		
The duration of storage of audit data is adequate to ensure recognition of security incidents and subsequent analysis of their occurrence, and will be a minimum of 30 days.	✓		
Auditable security events include, at a minimum: • Use of identification and authentication mechanisms. • Use of privilege mechanisms. • Introduction of "objects" into a user's address space. • Deletion of "objects." • Actions taken by security personnel and systems administrators.	✓		
For each recorded event, the audit trail includes the following information: • Date and time of the event. • Unique-user identification. • Type of event. • Success or failure of the event. • Terminal identification.	✓		
Auditing is enabled.	✓		
Critical system directories are audited.	✓		
INTEGRITY	**MET**	**NOT MET**	**NA**
All parts of the system (hardware, software, firmware, processes, data, and documentation) are protected in a verifiable manner against tampering, loss, or destruction throughout their lifetime.	✓		
Virus prevention measures commensurate with the level of risk identified in the risk analysis shall be employed to protect the integrity of the software and data.	✓		
GUIDANCE	**MET**	**NOT MET**	**NA**
No data is introduced into a system without designation of the classification or sensitivity of the data.	✓		
All critical or sensitive applications are properly identified.	✓		
AVAILABILITY OF SERVICE	**MET**	**NOT MET**	**NA**
Information in the system is available when needed.	✓		
The system provides a mechanism for controlling and managing consumption of disk space.	✓		
Preventative maintenance is performed on a schedule comparable to that recommended by the equipment's manufacturer.	✓		
The system provides a mechanism to support software and data backup and restoration. The mechanism incorporates synchronization points and allows recovery after a system failure or other discontinuity without a security compromise.	✓		
INCIDENT RESPONSE	**MET**	**NOT MET**	**NA**
Agencies review the susceptibility of their programs and functions to waste, loss, unauthorized use, and misappropriation. This review includes vulnerability assessments and equivalent reviews, such as audits.	✓		
The system actively prevents infection of malicious code by only allowing the installation and use of authorized software that is free of malicious code, and by executing effective antiviral software on all software on the system upon installation of any software and on the entire system at least on a quarterly basis.	✓		
The system has the capability to identify and record unauthorized attempts to gain access.	✓		
Whenever a virus infection is detected, it should be reported to the information assurance security officer.	✓		
Controls exist to detect and/or prevent covert penetration attempts.	✓		
FIREWALLS	**MET**	**NOT MET**	**NA**
The firewall is configured to deny unauthorized access to all protected components.	✓		

Figure 5-1. Sample of a completed USAAC Form 106 (Continued)

Administrative access to the firewall from other than the console only occurs after successful strong authentication.	✓		
The firewall configuration explicitly states the host and network Internet protocol addresses for which access is allowed.	✓		
The firewall is capable of being configured to dynamically deny access to Internet protocol addresses based on anomalous behavior such as network flooding.	✓		
The firewall is capable of being configured to selectively manage traffic priority based on host or network Internet protocol addresses during high-traffic periods.	✓		
Firewall proxies are configured to deny access unless explicitly configured otherwise.	✓		
Specific proxy capabilities (e.g., a file transfer protocol pull) are explicitly defined and include the appropriate access controls.	✓		
FACILITY ACCESS CONTROLS	**MET**	**NOT MET**	**NA**
The facility housing computer equipment shall provide physical security mechanisms to restrict access.	✓		
The facility shall maintain an access roster at each facility entry point.	✓		
The facility shall maintain a cleared visitor roster or file of current visitation request forms.	✓		
Positive personnel identification measures (e.g., badge system, fingerprints) shall be in place.	✓		
All uncleared personnel granted facility access must be properly escorted and restricted to those areas necessary to complete their tasks. Sensitive information must be protected from unauthorized disclosure to such persons.	✓		
The information assurance security officer shall ensure that network interfaces (hardware connections) in the terminal area are physically protected as required to achieve a level of protection adequate to prevent disruption resulting from accidental causes.	✓		
Sensitive information must be processed, stored, or transmitted in spaces that are under exclusive control while operational.	✓		
All terminal areas shall be physically secured at the end of the day.	✓		
Access to the computer center, server, cable closets, etc., shall be limited to personnel who have a justifiable need for access.	✓		
When combination locks are used to control access to the computer resources, those locks shall be changed periodically and after the termination or reassignment of any employee.	✓		
When keys are used to control facility access, those keys shall be changed periodically and after the termination and/or reassignment of any employees.	✓		
Keys shall be formally signed out.	✓		
ENVIRONMENTAL CONTROLS	**MET**	**NOT MET**	**NA**
An uninterruptible power supply shall be provided to prevent loss of data during power interruptions.	✓		
An emergency power switch shall be in place in the computer center and clearly marked.	✓		
Security devices that limit the amount of damage caused by environmental disasters (e.g., fire and flood) shall exist in the computer areas (e.g., smoke and water detectors, fire extinguishers, sprinklers).	✓		
The fire detection system shall be tested periodically.	✓		
SOFTWARE AND DATA SECURITY	**MET**	**NOT MET**	**NA**
Only necessary trust relationships exist with other domains.	✓		
Access to all shared folders is restricted.	✓		

Figure 5-1. Sample of a completed USAAC Form 106 (Continued)

Proprietary software is protected against compromise.	✓		
Software is scanned for viruses before being introduced to the system.	✓		
DESIGNATED APPROVING AUTHORITY	**MET**	**NOT MET**	**NA**
A designated approving authority is designated as responsible for the overall security of the connected systems.	✓		
CERTIFIER	**MET**	**NOT MET**	**NA**
A certifier conducts a comprehensive evaluation of the technical and nontechnical security features of the connected systems to establish the extent to which the design and implementation meet the set of specified security requirements (e.g., the security policy).	✓		
ADMINISTRATOR	**MET**	**NOT MET**	**NA**
Security and system administrators ensure that the system security policy, as established by the designated approving authority, is implemented.	✓		
System administrators are certified.	✓		
REQUIREMENTS ANALYSIS	**MET**	**NOT MET**	**NA**
An analysis is performed to identify all security requirements for the entire life cycle of the system.	✓		
System boundaries and interfaces are defined to maximize the security of the system and minimize the threat from external sources.	✓		
RISK MANAGEMENT	**MET**	**NOT MET**	**NA**
A risk management program, approved by the designated approving authority, determines the most economical way of providing a reasonable assurance of information security protection.	✓		
A program exists to periodically identify, measure, control, and minimize uncertain events affecting system resources.	✓		
SYSTEM DEVELOPMENT	**MET**	**NOT MET**	**NA**
For any system that will handle sensitive unclassified or unclassified data, the entire system development life cycle is controlled to ensure its integrity at all levels, including the use of "best commercial practices."	✓		
TESTING	**MET**	**NOT MET**	**NA**
Before a new or modified automated information system is placed into production, its controls are tested to prove that they operate as intended and to ensure the established minimum security requirements are met.	✓		
TRAINING AND AWARENESS	**MET**	**NOT MET**	**NA**
If passwords are selected as the authentication mechanism for the system, users must be briefed on the following at the time of password issuance: • Password classification and exclusiveness. • Measures to safeguard "sensitive" passwords. • Prohibitions against disclosing passwords to other personnel. • Responsibilities for notifying the information assurance security officer of password misuse. • Password change procedures.	✓		
Individuals assigned primary responsibility for performing critical functions in support of the automated information system (e.g., system administration, security administration, system operations, programming) should have trained alternates who can perform these functions in the event the individual assigned primary responsibility is unavailable.	✓		
Agency's training practices shall be reviewed biennially to ensure that all agency personnel are familiar with requirements of the Privacy Act, with the agency's implementing regulation, and with special requirements of their specific jobs.	✓		
A security awareness training plan is in place and in use.	✓		
All information assurance and system administrator personnel have attended training required for security certification.	✓		
CONTINGENCY PLANS	**MET**	**NOT MET**	**NA**
The approved contingency plan shall be periodically tested.	✓		

Figure 5-1. Sample of a completed USAAC Form 106 (Continued)

The system has a tested contingency plan addressing full system restoration.	✓		
Another system can be used to avoid interruption of important processing if the system were destroyed or in need of repair.	✓		
Backups are made of critical applications on a regular basis.	✓		
Backups are stored offsite and the security posture of the offsite location is adequate for their storage.	✓		
Current contingency plans exist for the system that cover all anticipated emergencies, backups, and disaster recovery.	✓		
A current, tested, system emergency action plan exists and assigns clear responsibilities for actions to be taken during the emergency. These actions are listed in priority order. The emergency action plan is tested frequently.	✓		
A system backup plan exists that: • Identifies critical and vital files that must be backed up, including how the media containing those files are to be marked. • Identifies essential documentation that must be available in the event the primary processing site is unavailable. • Establishes the frequency of backups and rotation schedule of the backup media. • Provides for offsite storage of the backed up media and essential documentation. • Contains information relating to security of the backed up media, including its security while being transported to and from the offsite location. • Contains information regarding a backup computer facility.	✓		
A disaster recovery plan exists that: • Establishes evaluation criteria for determining the extent of disruption of functions and operations. • Identifies backup processing sites. • Covers the safeguarding or destruction of sensitive unclassified information in the event that the primary site must be evacuated. • Provides detailed plans for the movement of personnel and the backup media and documentation to the backup processing site. • Provides guidance for testing the plan.	✓		
The contingency plan has been tested in the last year and has the following characteristics: • Deals with less than catastrophic occurrences as well as major catastrophic events. • Clearly and unambiguously assigns responsibilities. • Clearly outlines the amount of downtime that can be tolerated before disaster is declared. • The system has adequate capability to recognize and contain incidental releases of sensitive unclassified or unclassified information on to inappropriate or incorrect network or system.	✓		
PERSONNEL SECURITY	**MET**	**NOT MET**	**NA**
All personnel associated with the system are subject to a personnel security background investigation and have appropriate clearance for the data and systems accessed.	✓		
A list is maintained of all persons who have access to the areas where the systems are located, and the list shows the level of access of each individual and is kept current at all times.	✓		
All personnel having unescorted privileges to the systems areas possess a clearance or access authorization equal to or higher than the highest classification of all categories of information on the systems.	✓		
Maintenance and cleaning personnel are cleared, or if uncleared, are escorted.	✓		
All personnel receive appropriate security briefings upon arrival and before beginning their assigned duties.	✓		
Passwords are changed or deleted for individuals when: • Their access is withdrawn for any reason. • There has been a compromise or suspected compromise of the password. • A maximum of 6 months has elapsed since the last change.	✓		
Corrective action has been taken for all security violations reported within the past year.	✓		
Upon termination of job function, access is removed, personnel are debriefed, required to return all material related to operations, and required to execute a security termination statement.	✓		

Figure 5-1. Sample of a completed USAAC Form 106 (Continued)

PHYSICAL SECURITY	MET	NOT MET	NA
All removable media are controlled at the highest classification level or sensitivity and criticality category of information on the media.	✓		
Unencrypted sensitive unclassified lines do not exist, or if they do, continual surveillance and protection are provided.	✓		
Access to the system patch panel is controlled.	✓		
Access to equipment locations is controlled during working hours and after working hours.	✓		
An individual cannot gain access to the system's working areas during or after working hours without detection.	✓		
A log is maintained of all personnel who enter or leave the building after normal duty hours, and the log indicates the specific workspaces accessed.	✓		
The facility is equipped with a fire, smoke detection, suppression, and alarm system that is tested periodically.	✓		
A media library exists and is protected against unauthorized access.	✓		
Positive security controls are maintained over all components of the system at all times.	✓		
ADMINISTRATIVE (PROCEDURAL) SECURITY	**MET**	**NOT MET**	**NA**
Power distribution panels and circuit breaker panels are clearly marked to indicate which switches control each outlet or piece of equipment.	✓		
A log is maintained of all hardware servicing and modifications.	✓		
Access to programs and software applications are restricted on a need-to-know basis.	✓		
All items of hardware are adequately identified and an inventory is kept.	✓		
Passwords are disclosed only to their intended users.	✓		
An inventory is maintained of all system software that also records the software's location.	✓		
Procedures exist to recover a deleted data file.	✓		
Memorandums of understanding exist for all site installation communications.	✓		
Controls exist to ensure that data submitted for input originated from an approved source.	✓		
All auto-answer modems used are specifically approved by the designated approving authority.	✓		
EMANATIONS SECURITY	**MET**	**NOT MET**	**NA**
A TEMPEST Countermeasure Review has been submitted, as applicable.	✓		
POLICY DOCUMENTATION	**MET**	**NOT MET**	**NA**
An explicit and well-defined security policy is enforced by the system. The security policy of the system establishes goals for safeguarding the confidentiality, integrity, and availability of all components of and data handled by the system and procedures for attaining those goals.	✓		
The personnel security policy of the system ensures that all personnel responsible for the design, development, operation, maintenance, or administration are qualified.	✓		
A security analysis is part of the system's documentation.	✓		
The security architecture is part of the system's documentation.	✓		
A risk assessment is part of the system's documentation.	✓		

Figure 5-1. Sample of a completed USAAC Form 106 (Continued)

System security standing operating procedures is part of the system's documentation.	✓		
The system's interface specification describes the security required for both internal and external interfaces of the system.	✓		
The system's security test and evaluation plan fully describes how the security features of the system will be tested.	✓		
CERTIFICATION AND ACCREDITATION PACKAGE	**MET**	**NOT MET**	**NA**
Documentation proves that the security specification, design, and implementation of the system are sufficient to fulfill the security policies of the system.	✓		
Accreditation of the system under consideration includes a memorandum of agreement involving all other systems under another designated approving authority directly connected to the system under consideration.	✓		
The certification and accreditation package is updated at least every 3 years.	✓		
The accreditation of the system is supported by a certification plan, an evaluation of security safeguards, a risk assessment of the system in its operational environment, and a certification report.	✓		

REMARKS:

USAAC Form 106, 1 Apr 2005 Page 8 of 8

Figure 5-1. Sample of a completed USAAC Form 106 (Continued)

Appendix A
References

Section I
Required Publications

AR 25-2
Information Assurance. (Cited in paras 4-2g(4), 4-3i, 4-3r(5), 5-1, 5-1b(1), and 6-2.) (www.usapa.army.mil)

AR 380-53
Information Systems Security Monitoring. (Cited in para 4-3i.) (www.usapa.army.mil)

AR 380-67
Department of the Army Personnel Security Program (Cited in para 4-2g(4).) (www.usapa.army.mil)

CSC-STD-002-85
Department of Defense Password Management Guideline. (Cited in para 4-3r(5).) (www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.pdf)

DODI 5200.40
DOD Information Technology Security Certification and Accreditation Process (DITSCAP). (Cited in paras 2-4b and 5-1a.) (www.dtic.mil/whs/directives)

FIPS Pub 140-2
Security Requirements for Crypographic Modules. (Cited in para 4-3n.) (www.itl.nist.gov/fipspubs)

NSTISSI 4009
National Information Systems Security (INFOSEC) Glossary. (Cited in paras 3-3a and 3-4a.) (www.dss.mil/infoas)

Section II
Related Publications

AR 25-1
Army Knowledge Management and Information Technology Management. (www.usapa.army.mil)

AR 25-55
The Department of the Army Freedom of Information Act Program. (www.usapa.army.mil)

AR 380-5
Department of the Army Information Security Program. (www.usapa.army.mil)

FM 3-13
Information Operations: Doctrine, Tactics, Techniques, and Procedures. (www.tradoc.army.mil)

JCS Pub 3-13
Joint Doctrine for Information Operations. (www.dtic.mil/doctrine/s_index.html)

Section III
Prescribed Form

USAAC Form 106
Security Requirements Checklist. (Prescribed in para 5-3c.)

Glossary

Section I
Abbreviations

ACERT
Army Computer Emergency Response Team

AIS
automated information system

CA
Certification Authority

C&A
certification and accreditation

COMPUSEC
computer security

COMSEC
communications security

DA
Department of the Army

DAA
designated approving authority

DII
Defense Information Infrastructure

DITSCAP
Department of Defense Information Technology Security Certification and Accreditation Process

DMZ
demilitarized zone

DOD
Department of Defense

IA
information assurance

IAM
information assurance manager

IANM
information assurance network manager

IAPM
information assurance program manager

IASO
information assurance security officer

IATO
interim authority to operate

INFOSEC
information security

IS
information system

IT
information technology

LIASO
local information assurance security officer

NIPRNET
Unclassified but Sensitive Internet Protocol Router Network

NSA
National Security Agency

PM
program manager

SA
system administrator

SBU
sensitive but unclassified

SETAP
Security Education, Training, and Awareness Program

SIPRNET
Secret Internet Protocol Router Network

SOW
statement of work

SSAA
system security authorization agreement

USAAC
United States Army Accessions Command

WAN
wide area network

Section II
Terms

NOTE: These terms are taken from JCS Pub 3-13.

information assurance
Information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

information system
The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.